On Cyclotomic Polynomials with ± 1 Coefficients

Peter Borwein and Kwok-Kwong Stephen Choi

CONTENTS

Research of P. Borwein is supported, in part, by NSERC of Canada.

K.-K. Choi is a Pacific Institute of Mathematics Postdoctoral Fellow and the Institute's support is gratefully acknowledged.

Keywords: Cyclotomic polynomials, Mahler measure, Littlewood polynomials

Mathematics Subject Classification (1991): Primary 11R09; Secondary: 11Y99

We characterize all cyclotomic polynomials of even degree with coefficients restricted to the set $\{+1, -1\}$. In this context a cyclotomic polynomial is any monic polynomial with integer coefficients and all roots of modulus 1. *Inter alia* we characterize all cyclotomic polynomials with odd coefficients.

The characterization is as follows. A polynomial P(x) with coefficients ± 1 of even degree $N-1$ is cyclotomic if and only if

$$P(x) = \pm \Phi_{p_1}(\pm x)\, \Phi_{p_2}(\pm x^{p_1}) \cdots \Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes, not necessarily distinct, and where $\Phi_p(x) := (x^p - 1)/(x-1)$ is the p-th cyclotomic polynomial.

We conjecture that this characterization also holds for polynomials of odd degree with ± 1 coefficients. This conjecture is based on substantial computation plus a number of special cases.

Central to this paper is a careful analysis of the effect of Graeffe's root squaring algorithm on cyclotomic polynomials.

1. INTRODUCTION

We are interested in studying polynomials with coefficients restricted to the set $\{+1, -1\}$. This particular set of polynomials has drawn much attention and there are a number of difficult old questions concerning it. Littlewood [1968] raised a number of these questions and so we call these polynomials *Littlewood polynomials* and denote them by $\mathcal{L}$. A Littlewood polynomial of degree n has L_2 norm on the unit circle equal to $\sqrt{n+1}$. Many of the questions raised concern comparing the behavior of these polynomials in other norms to the L_2 norm. One of the older and more intriguing of these asks whether such polynomials can be "flat". Specifically, do there exist two positive constants C_1 and C_2 so that for each n there is a Littlewood polynomial of degree n with

$$C_1\sqrt{n+1} < |p(z)| < C_2\sqrt{n+1}$$

for each z of modulus 1? This problem, which has been open for more than forty years, is discussed in [Borwein 1998], where there is an extensive bibliography. The upper bound is satisfied by the so-called Rudin–Shapiro polynomials. It is still unknown whether there is a sequence satisfying just the lower bound (this problem has been called one of the "very hardest problems in combinatorial optimization").

The size of the L_p norm of Littlewood polynomials has been studied from a number of points of view. The problem of minimizing the L_4 norm (or equivalently of maximizing the so-called "merit factor") has also attracted a lot of attention.

In particular, can Littlewood polynomials of degree n have L_4 norm asymptotically close to $\sqrt{n+1}$? This too is still open and is discussed in [Borwein 1998].

Mahler [1963] raised the question of maximizing the Mahler measure of Littlewood polynomials. The Mahler measure is just the L_0 norm on the circle and one would expect this to be closely related to the minimization problem for the L_4 norm above. Of course the minimum possible Mahler measure for a Littlewood polynomial is 1 and this is achieved by any cyclotomic polynomial. In this paper we define a cyclotomic polynomial as any monic polynomial with integer coefficients and all roots of modulus 1, and denote by $\Phi_n(x)$ *the* n-th irreducible cyclotomic polynomial, that is, the minimum polynomial of a primitive n-th root of unity.

This paper addresses the question of characterizing the cyclotomic Littlewood polynomials of even degree. Specifically, we show that a polynomial $P(x)$ with coefficients ± 1 of even degree $N-1$ is cyclotomic if and only if

$$P(x) = \pm\Phi_{p_1}(\pm x)\,\Phi_{p_2}(\pm x^{p_1})\cdots\Phi_{p_r}(\pm x^{p_1 p_2\cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes (not necessarily distinct). The "if" part is obvious since $\Phi_{p_i}(x)$ has coefficients ± 1.

We also give an explicit formula for the number of such polynomials.

This analysis is based on a careful treatment of Graeffe's root squaring algorithm. It transpires that all cyclotomic Littlewood polynomials of a fixed degree have the same fixed point on iterating Graeffe's root squaring algorithm. This also allows us to characterize all cyclotomic polynomials with odd coefficients.

Substantial computations, as well as a number of special cases, lead us to conjecture that the above characterization of cyclotomic Littlewood polynomials of even degree also holds for odd degree. One of the cases we can handle is when N is a power of 2.

It is worth commenting on the experimental aspects of this paper. (As is perhaps usual, much of this is carefully erased in the final exposition). It is really the observation that the cyclotomic Littlewood polynomials can be explicitly constructed essentially by inverting Graeffe's root squaring algorithm that is critical. This allows for computation over all cyclotomic Littlewoods up to degree several hundred (with exhaustive search failing far earlier), a construction which is of interest in itself. Indeed it was these calculations that allowed for the conjectures of the paper and suggested the route to some of the results.

The paper is organized as follows. Section 2 examines cyclotomic polynomials with odd coefficients. Section 3 looks at cyclotomic Littlewood polynomials with a complete analysis of the even degree case. The last section presents some numerical evidence and other evidence to support the conjecture that the odd case behaves like the even case.

2. CYCLOTOMIC POLYNOMIALS WITH ODD COEFFICIENTS

In this section, we discuss the factorization of cyclotomic polynomials with odd coefficients as a product of irreducible cyclotomic polynomials. To do this, we first consider the factorization over $\mathbb{Z}_p[x]$, where p is a prime number. The most useful case is $p = 2$ because every Littlewood polynomial reduces to the Dirichlet kernel

$$1 + x + \cdots + x^{N-1}$$

in $\mathbb{Z}_2[x]$. In $\mathbb{Z}_p[x]$, $\Phi_n(x)$ is no longer irreducible in general but $\Phi_n(x)$ and $\Phi_m(x)$ are still relatively prime to each other.

Lemma 2.1. *Suppose n and m are distinct positive integers relatively prime to p. Then $\Phi_n(x)$ and $\Phi_m(x)$ are relatively prime in $\mathbb{Z}_p[x]$.*

Proof. Suppose e and f are the smallest positive integers such that

$$p^e \equiv 1 \pmod{n} \quad \text{and} \quad p^f \equiv 1 \pmod{m}.$$

Let F_{p^k} be the field of order p^k. Then F_{p^e} contains exactly $\varphi(n)$ elements of order n and over $\mathbb{Z}_p$, $\Phi_n(x)$ is a product of $\varphi(n)/e$ irreducible factors of degree e and each irreducible factor is a minimal polynomial for an element in F_{p^e} of order n over $\mathbb{Z}_p$; see [Lidl and Niederreiter 1983]. So $\Phi_n(x)$ and $\Phi_m(x)$ cannot have a common factor in $\mathbb{Z}_p[x]$ since their irreducible factors are minimal polynomials of different orders. This proves our lemma. □

The following lemma tells which $\Phi_m(x)$ can possibly be factors of polynomials with odd coefficients.

Lemma 2.2. *Suppose $P(x)$ is a polynomial with odd coefficients of degree $N-1$. If $\Phi_m(x)$ divides $P(x)$, then m divides $2N$.*

Proof. Since $\Phi_m(x)$ divides $P(x)$, so $\Phi_m(x)$ also divides $P(x)$ in $\mathbb{Z}_2[x]$. However, in $\mathbb{Z}_2[x]$, $P(x)$ equals to $1+x+\cdots+x^{N-1}$ and can be factored as

$$P(x) = \Phi_1(x)^{-1} \prod_{d\,|\,M} \Phi_d^{2^t}(x), \tag{2–1}$$

where $N = 2^t M$, $t \geq 0$ and M is odd. In view of Lemma 2.1, $\Phi_{d_1}(x)$ and $\Phi_{d_2}(x)$ are relatively prime in $\mathbb{Z}_2[x]$ if d_1 and d_2 are distinct odd integers. So if m is odd, then $\Phi_m(x)$ is a factor in the right hand side of (2–1) and hence $m = d$ for some $d\,|\,M$. On the other hand, if m is even and $m = 2^l m'$ where $l \geq 1$ and m' is odd, then

$$\Phi_m(x) = \Phi_{2m'}(x^{2^{l-1}}) = \Phi_{m'}(x^{2^{l-1}}) = \Phi_{m'}(x)^{2^{l-1}}$$

in $\mathbb{Z}_2[x]$. Thus, in view of (2–1), we must have $m' = d$ for $d\,|\,M$ and $l \leq t+1$. Hence in both cases we have m divides $2N$. □

In view of Lemma 2.2, every cyclotomic polynomial, $P(x)$, with odd coefficients of degree $N-1$ can be written as

$$P(x) = \prod_{d|2N} \Phi_d^{e(d)}(x), \tag{2–2}$$

where the $e(d)$ are nonnegative integers.

For each prime p let T_p be the operator defined over all monic polynomials in $\mathbb{Z}[x]$ by

$$T_p[P(x)] := \prod_{i=1}^{N} (x - \alpha_i^p)$$

for every $P(x) = \prod_{i=1}^N (x-\alpha_i)$ in $\mathbb{Z}[x]$. By Newton's identities [Borwein and Erdélyi 1995, p. 5], $T_p[P(x)]$ is also a monic polynomial in $\mathbb{Z}[x]$. We extend T_p to be defined over the quotient of two monic polynomials in $\mathbb{Z}[x]$ by $T_p[(P/Q)(x)] := T_p[P(x)]/T_P[Q(x)]$. This operator obviously takes a polynomial to the polynomial whose roots are the p-th powers of the roots of P. Also we let M_p be the natural projection from $\mathbb{Z}[x]$ onto $\mathbb{Z}_p[x]$:

$$M_p[P(x)] = P(x) \pmod{p}.$$

Lemma 2.3. *Suppose that n is a positive integer relatively prime to p and $i \geq 2$. Then*

(i) $T_p[\Phi_n(x)] = \Phi_n(x)$,
(ii) $T_p[\Phi_{pn}(x)] = \Phi_n(x)^{p-1}$,
(iii) $T_p[\Phi_{p^i n}(x)] = \Phi_{p^{i-1}n}(x)^p$.

Proof. (i) is trivial because if $(n,p) = 1$ then T_p just permutes the roots of $\Phi_n(x)$. To prove (ii) and (iii), we consider

$$\begin{aligned} T_p[P(x^p)] &= T_p\left[\prod_{j=1}^{N}(x^p - \alpha_i)\right] \\ &= T_p\left[\prod_{j=1}^{N}\prod_{l=1}^{p}(x - e^{2\pi il/p}\alpha_i^{1/p})\right] \\ &= \prod_{j=1}^{N}\prod_{l=1}^{p}(x-\alpha_i) \\ &= P(x)^p. \end{aligned}$$

Thus (ii) and (iii) follow from (i) and the equalities $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ and $\Phi_{p^i n}(x) = \Phi_{p^{i-1}n}(x^p)$ [Hungerford 1974, § 5.8]. □

When $P(x)$ is cyclotomic, the iterates $T_p^n[P(x)]$ converge in a finite number of steps to a fixed point of T_p and we define this to be the fixed point of $P(x)$ with respect to T_p.

Lemma 2.4. *If $P(x)$ is a monic cyclotomic polynomial in $\mathbb{Z}[x]$, then*

$$M_p[T_p[P(x)]] = M_p[P(x)], \tag{2–3}$$

in $\mathbb{Z}_p[x]$.

Proof. Since both T_p and M_p are multiplicative, it suffices to consider the primitive cyclotomic polynomials $\Phi_n(x)$. Let n be an integer relatively prime to p. Then (2–3) is true for $P(x) = \Phi_n(x)$ by (i) of Lemma 2.3. For $P(x) = \Phi_{pn}(x)$, we have

$$M_p[T_p[\Phi_{pn}(x)]] = M_p[\Phi_n(x)^{p-1}] = M_p[\Phi_n(x)]^{p-1}$$

by (ii) of Lemma 2.3. However,

$$M_p[\Phi_{pn}(x)] = \frac{M_p[\Phi_n(x^p)]}{M_p[\Phi_n(x)]} = \frac{M_p[\Phi_n](x^p)}{M_p[\Phi_n(x)]} = M_p[\Phi_n(x)]^{p-1}$$

in $\mathbb{Z}_p[x]$. This proves that (2–3) is also true for $P(x) = \Phi_{pn}(x)$. Finally, $P(x) = \Phi_{p^i n}(x)$ implies

$$\begin{aligned} M_p[T_p[\Phi_{p^i n}(x)]] &= M_p[\Phi_{p^{i-1}n}(x)^p] \\ &= M_p[\Phi_{p^{i-1}n}(x^p)] \\ &= M_p[\Phi_{p^i n}(x)] \end{aligned}$$

by (iii) of Lemma 2.3. This completes the proof of our lemma. □

Lemma 2.4 shows that $T_p[P(x)] = T_p[Q(x)]$ implies $M_p[P(x)] = M_p[Q(x)]$. The next result shows that the converse is also true.

Theorem 2.5. *$P(x)$ and $Q(x)$ are monic cyclotomic polynomials in $\mathbb{Z}[x]$ and $M_p[P(x)] = M_p[Q(x)]$ in $\mathbb{Z}_p[x]$ if and only if both $P(x)$ and $Q(x)$ have the same fixed point with respect to iteration of T_p.*

Proof. Suppose

$$P(x) = \prod_{d\in\mathcal{D}} \Phi_d^{e(d)}(x)\,\Phi_{pd}^{e(pd)}(x)\cdots\Phi_{p^t d}^{e(p^t d)}(x)$$

and

$$Q(x) = \prod_{d\in\mathcal{D}} \Phi_d^{e(d)'}(x)\,\Phi_{pd}^{e(pd)'}(x)\cdots\Phi_{p^t d}^{e(p^t d)'}(x),$$

where $t, e(j), e(j)' \geq 0$ and $\mathcal{D}$ is a set of positive integers relatively prime to p. Then using parts (i)–(iii) of Lemma 2.3, we have for $l \geq t$

$$\begin{aligned} T_p^l[P(x)] &= \prod_{d\in\mathcal{D}} \Phi_d(x)^{f(d)}, \\ T_p^l[Q(x)] &= \prod_{d\in\mathcal{D}} \Phi_d(x)^{f(d)'}, \end{aligned} \tag{2–4}$$

where

$$\begin{aligned} f(d) &= e(d) + (p-1)\sum_{j=1}^{t} p^{j-1} e(p^j d), \\ f(d)' &= e(d)' + (p-1)\sum_{j=1}^{t} p^{j-1} e(p^j d)'. \end{aligned}$$

From Lemma 2.4, we have

$$\begin{aligned} M_p[T_p^l[P(x)]] &= M_p[P(x)] = M_p[Q(x)] \\ &= M_p[T_p^l[Q(x)]], \end{aligned}$$

for any $l \geq t$. From this and (2–4),

$$\prod_{d\in\mathcal{D}} M_p[\Phi_d(x)]^{f(d)} = \prod_{d\in\mathcal{D}} M_p[\Phi_d(x)]^{f(d)'}.$$

However, with Lemma 2.1, we know that $M_p[\Phi_d(x)]$ and $M_p[\Phi_{d'}(x)]$ are relatively prime if $d \neq d'$. So we must have $f(d) = f(d)'$ for all $d \in \mathcal{D}$ and hence from (2–4), $P(x)$ and $Q(x)$ have the same fixed point with respect to T_p. □

From Theorem 2.5, we can characterize the monic cyclotomic polynomials by their images in $\mathbb{Z}_p[x]$ under the projection M_p. They all have the same fixed point under T_p. In particular, when $p = 2$ we have:

Corollary 2.6. *All monic cyclotomic polynomials with odd coefficients of the degree $N-1$ have the same fixed point under iteration of T_2. Specifically, if $N = 2^t M$ where $t \geq 0$ and M is odd then the fixed point occurs at the $(t+1)$-th step of the iteration and equals*

$$(x^M - 1)^{2^t}(x-1)^{-1}.$$

Proof. The first part follows directly from Theorem 2.5 and the fact that

$$M_2[P(x)] = 1 + x + \cdots + x^{N-1}$$

in $\mathbb{Z}_2[x]$ if $P(x)$ is a monic polynomial with odd coefficients of degree $N-1$. If $N = 2^t M$, then from (2–2),

$$P(x) = \prod_{d\mid M} \Phi_d^{e(d)}(x)\,\Phi_{2d}^{e(2d)}(x)\cdots\Phi_{2^{t+1}d}^{e(2^{t+1}d)}(x).$$

Over $\mathbb{Z}_2[x]$,

$$1 + x + \cdots + x^{N-1} = \Phi_1(x)^{-1}\prod_{d\mid M}\Phi_d^{2^t}(x),$$

so

$$\begin{aligned} f(d) &= e(d) + \sum_{i=1}^{t+1} 2^{i-1} e(2^i d) \\ &= \begin{cases} 2^t & \text{for } d \mid M,\ d > 1, \\ 2^t - 1 & \text{for } d = 1. \end{cases} \end{aligned} \tag{2–5}$$

Therefore, from (2–5) and Lemma 2.3,

$$T_2^{t+1}[P(x)] = \prod_{d|M} \Phi_d^{f(d)}(x) = \Phi_1(x)^{-1} \prod_{d|M} \Phi_d^{2^t}(x)$$
$$= (x^M - 1)^{2^t}(x-1)^{-1}. \qquad \square$$

Corollary 2.6, when N is odd ($t = 0$), shows that $T_2[P(x)]$ equals $1 + x + \cdots + x^{N-1}$ for all cyclotomic polynomials with odd coefficients. From (2–2) and (2–5), we then have the following characterization of cyclotomic polynomials with odd coefficients.

Corollary 2.7. *Let $N = 2^t M$ with $t \geq 0$ and M odd. A polynomial, $P(x)$, with odd coefficients of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \prod_{d|M} \Phi_d^{e(d)}(x)\, \Phi_{2d}^{e(2d)}(x) \cdots \Phi_{2^{t+1}d}^{e(2^{t+1}d)}(x),$$

and the $e(d)$ satisfy the condition (2–5).

Furthermore, if N is odd, then any polynomial, $P(x)$, with odd coefficients of even degree $N-1$ is cyclotomic if and only if

$$P(x) = \prod_{\substack{d|N \\ d>1}} \Phi_d^{e(d)}(\pm x),$$

where the $e(d)$ are nonnegative integers.

Corollary 2.7 allows us to compute the number of cyclotomic polynomials with odd coefficients. Let $B(n)$ be the number of partitions of n into a sum of terms of the sequence $\{1, 1, 2, 4, 8, 16, \ldots\}$. Then $B(n)$ has generating function

$$F(x) = (1-x)^{-1} \prod_{k=0}^{\infty} (1 - x^{2^k})^{-1}.$$

Corollary 2.8. *Let $N = 2^t M$ with $t \geq 0$ and M odd. The number of cyclotomic polynomials with odd coefficients of degree $N-1$ is*

$$C(N) = B(2^t)^{d(M)-1} B(2^t - 1), \tag{2–6}$$

where $d(M)$ denotes the number of divisors of M. Furthermore,

$$\log C(N) \sim \left(\tfrac{1}{2} t^2 \log 2\right)(d(M) - 1) + \frac{(\log(2^t - 1))^2}{\log 4}. \tag{2–7}$$

Proof. Formula (2–6) follows from (2–5) and Corollary 2.7. To prove (2–7), we use de Bruijn's asymptotic estimation for $B(n)$ in [de Bruijn 1948]:

$$B(n) \sim \exp((\log n)^2/\log 4).$$

Now (2–7) follows from this and (2–6). $\square$

3. CYCLOTOMIC LITTLEWOOD POLYNOMIALS

We now specialize the discussion to the case where the coefficients are all $+1$ or -1.

One natural way to build up Littlewood polynomial of higher degree is as follows: if $P_1(x)$ and $P_2(x)$ are Littlewood polynomials and $P_1(x)$ is of degree $N-1$ then $P_1(x)P_2(x^N)$ is a Littlewood polynomial of higher degree. In this section, we show that this is the only way to produce cyclotomic Littlewood polynomials, at least for even degree.

Proving this is equivalent to showing that the coefficients of $P(x)$ are "periodic" in the sense that if $P(x) = \sum_{n=0}^{N-1} a_n x^n$, then there is a "period" i such that $a_{li+n} = a_{li}$ for all $1 \leq n \leq i-1$ and $0 \leq l \leq N/i - 1$. This is our Theorem 3.3 below.

Suppose $P(x) = \sum_{n=0}^{N-1} a_n x^n$ is a cyclotomic polynomial in $\mathcal{L}$ and let S_k be the sum of the k-th powers of all the roots of $P(x)$. Since $P(x)$ is cyclotomic, we have $x^{N-1}P(1/x) = \pm P(x)$. Thus it follows from Newton's identities that

$$S_k + a_1 S_{k-1} + \cdots + a_{k-1} S_1 + k a_k = 0 \tag{3–1}$$

for $k \leq N-2$. We may further assume that $a_0 = a_1 = 1$ by replacing $P(x)$ by $-P(x)$ or $P(-x)$ if necessary. We now let

$$a_0 = a_1 = \cdots = a_{i-1} = 1 \quad \text{and} \quad a_i = -1,$$

for some integer $i \geq 2$. From (3–1), we have

$$S_1 = -a_1 = -1.$$

We claim that

$$\begin{aligned} s_1 = S_2 = \cdots = S_{i-1} &= -1, \\ S_i &= 2i - 1. \end{aligned} \tag{3–2}$$

Suppose $S_1 = \cdots = S_j = -1$ for $j < i-1$. Then from (3–1) again,

$$\begin{aligned} S_{j+1} &= -a_1 S_j - \cdots - a_j S_1 - (j+1) a_{j+1} \\ &= j - (j+1) = -1. \end{aligned}$$

So $S_1 = \cdots = S_{i-1} = -1$. Similarly, from (3–1),

$$S_i = -a_1 S_{i-1} - \cdots - a_{i-1} S_1 - i a_i = 2i - 1.$$

Lemma 3.1. *Let $2 \le k \le \frac{N-1}{i} - 1$ and suppose $a_{li+n} = a_{li}$ for $1 \le n \le i-1$ and $0 \le l \le k-2$. Then*

$$\sum_{l=0}^{k-2} a_{li}\left(S_{(k-l)i+j+1} - S_{(k-l-1)i+j+1}\right) + (ki+j+1)(a_{ki+j+1} - a_{ki+j}) + \sum_{n=0}^{i-1} a_{(k-1)i+n}(S_{i+j-n+1} - S_{i+j-n}) = 0 \quad \text{(3–3)}$$

for $0 \le j \le i-2$.

Proof. Suppose $0 \le j \le i-2$. From (3–1) and (3–2) we have

$$\begin{aligned} 0 &= \sum_{l=0}^{k-1}\sum_{n=0}^{i-1} a_{li+n} S_{(k-l)i+j-n} + \sum_{n=0}^{j-1} a_{ki+n} S_{j-n} + (ki+j)a_{ki+j} \\ &= \sum_{l=0}^{k-2} a_{li} \sum_{n=0}^{i-1} S_{(k-l)i+j-n} + \sum_{n=0}^{i-1} a_{(k-1)i+n} S_{i+j-n} - \sum_{n=0}^{j} a_{ki+n} + (ki+j+1)a_{ki+j}. \end{aligned} \quad \text{(3–4)}$$

Similarly,

$$0 = \sum_{l=0}^{k-2} a_{li} \sum_{n=0}^{i-1} S_{(k-l)i+j-n+1} + \sum_{n=0}^{i-1} a_{(k-1)i+n} S_{i+j-n+1} - \sum_{n=0}^{j} a_{ki+n} + (ki+j+1)a_{ki+j+1}. \quad \text{(3–5)}$$

Hence, on subtracting (3–5) from (3–4), we have

$$0 = \sum_{l=0}^{k-2} a_{li}\left(S_{(k-l)i+j+1} - S_{(k-l-1)i+j+1}\right) + (ki+j+1)(a_{ki+j+1} - a_{ki+j}) + \sum_{n=0}^{i-1} a_{(k-1)i+n}(S_{i+j-n+1} - S_{i+j-n}).$$

This proves (3–3). □

Lemma 3.2. *Let $0 \le k \le \frac{N-1}{i} - 1$. Suppose $a_{li+n} = a_{li}$ for $1 \le n \le i-1$ and $0 \le l \le k$. Then*

$$S_{li+n} = -1 \quad \text{(3–6)}$$

for $1 \le n \le i-1$ and $0 \le l \le k$.

Proof. We prove this by induction on k. We have proved that (3–6) is true for $k = 0$. Suppose (3–6) is true for $k-1$. Then, for any $0 \le j \le i-2$,

$$\begin{aligned} 0 &= a_0(S_{ki+j+1} - S_{(k-1)i+j+1}) + a_{(k-1)i}\sum_{n=0}^{i-1}(S_{i+j-n+1} - S_{i+j-n}) \\ &= S_{ki+j+1} + 1 + a_{(k-1)i}(S_{i+j+1} - S_{j+1}) \\ &= S_{ki+j+1} + 1, \end{aligned}$$

by (3–3). Hence $S_{ki+j+1} = -1$ for $0 \le j \le i-2$. □

Theorem 3.3. *Suppose N is odd. If $a_0 = a_1 = \cdots = a_{i-1} = 1$ and $a_i = -1$, then*

$$a_{li+n} = a_{li}$$

for $1 \le n \le i-1$ and $0 \le l \le \frac{N}{i} - 1$.

Proof. We first show that $S_{2k} = -1$ for $1 \le k \le N-1$ and hence i is odd because $S_i = 2i-1$. Since N is odd, from Corollary 2.7,

$$P(x) = \prod_{d|N} \Phi_d^{e(d)}(x)\,\Phi_{2d}^{e(2d)}(x)$$

where $e(d) + e(2d) = 1$ if $d > 1$ and $e(1) = e(2) = 0$. If $1 \le k \le N-1$, then

$$\begin{aligned} S_{2k} &= \sum_{d|N} \left(e(d)C_d(2k) + e(2d)C_{2d}(2k)\right) \\ &= \sum_{d|N}(e(d) + e(2d))C_d(k) \\ &= \sum_{d|N} C_d(k) - C_1(k) \\ &= -1, \end{aligned} \quad \text{(3–7)}$$

where the Ramanujan sum, $C_d(k)$, is the sum of the k-th powers of the primitive d-th roots of unity and hence $\sum_{d|N} C_d(k)$ is the sum of k-th powers of the roots of $\prod_{d|N}\Phi_d(x) = x^N - 1$, which is equal to zero when $1 \le k \le N-1$.

We continue our proof by using induction on k. Suppose

$$a_{li+n} = a_{li}$$

for $1 \le n \le i-1$ and $0 \le l \le k-1$ where $1 \le k \le \frac{N-1}{i} - 1$. From Lemmas 3.1 and 3.2 we have

$$S_{ki+j+1} + 1 + (ki+j+1)(a_{ki+j+1} - a_{ki+j}) = 0 \quad \text{(3–8)}$$

and hence from (3–3) again

$$\begin{aligned}0 &= a_0(S_{(k+1)i+j+1}-S_{ki+j+1})+a_i(S_{ki+j+1}-S_{(k-1)i+j+1})\\ &\quad +a_{ki+j}(S_{i+1}-S_i)+a_{ki+j+1}(S_i-S_{i-1})\\ &\quad +((k+1)i+j+1)(a_{(k+1)i+j+1}-a_{(k+1)i+j})\\ &= (S_{(k+1)i+j+1}-2S_{ki+j+1}-1)+2i(a_{ki+j+1}-a_{ki+j})\\ &\quad +((k+1)i+j+1)(a_{(k+1)i+j+1}-a_{(k+1)i+j})\\ &= S_{(k+1)i+j+1}+1+2((k+1)i+j+1)(a_{ki+j+1}-a_{ki+j})\\ &\quad +((k+1)i+j+1)(a_{(k+1)i+j+1}-a_{(k+1)i+j}) \qquad (3\text{–}9)\end{aligned}$$

for $0 \le j \le i-2$. Suppose k is even. Then in view of (3–7), $S_{ki+j+1} = -1$ if j is odd and $S_{(k+1)i+j+1} = -1$ if j is even. So from (3–8) and (3–9), we have

$$a_{ki+j+1} = a_{ki+j}$$

for $j = 1, 3, \ldots, i-2$ and

$$-2(a_{ki+j+1} - a_{ki+j}) = a_{(k+1)i+j+1} - a_{(k+1)i+j} \qquad (3\text{–}10)$$

for $j = 0, 2, \ldots, i-3$. However, since the a_i's are $+1$ or -1, Equation (3–10) implies that

$$a_{ki+j+1} = a_{ki+j} \quad \text{and} \quad a_{(k+1)i+j+1} = a_{(k+1)i+j}$$

for $j = 0, 2, \ldots, i-3$. Hence $a_{ki+n} = a_{ki}$ for $n = 1, 2, \ldots, i-1$. The case of k odd can be proved in the same way. □

Theorem 3.4. *Suppose N is odd. A Littlewood polynomial, $P(x)$, of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \pm\Phi_{p_1}(\pm x)\,\Phi_{p_2}(\pm x^{p_1})\cdots\Phi_{p_r}(\pm x^{p_1p_2\cdots p_{r-1}}), \qquad (3\text{–}11)$$

where $N = p_1p_2\cdots p_r$ and the p_i are primes, not necessarily distinct.

Proof. It is clear that if $P(x)$ is of the form (3–11), then $P(x)$ is a cyclotomic Littlewood polynomial. Conversely, suppose $P(x)$ is a cyclotomic Littlewood polynomial. As before we may assume that $a_0 = a_1 = \cdots = a_{i-1} = 1$ and $a_i = -1$. We prove our result by induction on N. From Theorem 3.3, we have $P(x) = P_1(x)P_2(x^i)$, where $P_1(x) = 1+x+\cdots+x^{i-1}$ and $P_2(x)$ is a cyclotomic Littlewood polynomial of degree less than $N-1$. By induction, $P_1(x)$ and $P_2(x)$ are of the form (3–11) and hence so is $P(x)$ because the degree of $P_1(x)$ is $i-1$. □

Corollary 3.5. *Suppose N is odd. Then $P(x)$ is cyclotomic in $\mathcal{L}$ of degree $N-1$ if and only if*

$$P(x) = \pm\prod_{i=1}^{t}\frac{x^{N_i}+(-1)^{\varepsilon+i}}{x^{N_{i-1}}+(-1)^{\varepsilon+i}}$$

where $\varepsilon = 0$ or 1, $N_0 = 1, N_t = N$ and N_{i-1} is a proper divisor of N_i for $i = 1, 2, \ldots, t$.

Proof. Without loss of generality, we may assume that $P(x) = 1 + x + a_2x^2 + \cdots$. From Theorem 3.4, $P(x)$ is cyclotomic in $\mathcal{L}$ if and only if

$$\begin{aligned}P(x) &= \Phi_{p_1}(x)\,\Phi_{p_2}(\pm x^{p_1})\cdots\Phi_{p_r}(\pm x^{p_1\cdots p_{r-1}})\\ &= \Phi_{p_1}(x)\cdots\Phi_{p_{n_1}}(x^{p_1\cdots p_{n_1-1}})\\ &\quad\times\Phi_{p_{n_1+1}}(-x^{p_1\cdots p_{n_1}})\cdots\Phi_{p_{n_2}}(-x^{p_1\cdots p_{n_2-1}})\\ &\quad\times\cdots\\ &\quad\times\Phi_{p_{n_{t-1}+1}}((-1)^{t-1}x^{p_1\cdots p_{n_{t-1}}})\cdots\\ &\qquad\qquad\Phi_{p_{n_t}}((-1)^{t-1}x^{p_1\cdots p_{n_t-1}}),\end{aligned}$$

where $N = p_1\cdots p_{n_t}$. Since $\Phi_p(x) = (x^p-1)/(x-1)$, the preceding equation becomes

$$P(x) = \prod_{i=1}^{t}\frac{x^{N_i}+(-1)^i}{x^{N_{i-1}}+(-1)^i},$$

where $N_0 = 1$ and $N_i = p_1\cdots p_{n_i}$ for $i = 1, \ldots, t$. This proves our corollary. □

Using Corollary 3.5, we can count the number of cyclotomic Littlewood polynomials of given even degree. For any positive integers N and t, define

$$\begin{aligned}r(N,t) := \#\{(N_1, N_2, \ldots, N_t) : N_1 \mid N_2 \mid \cdots \mid N_t,&\\ 1 < N_1 < N_2 < \cdots < N_t = N\};&\end{aligned}$$

and for $i \ge 1$,

$$d_i(N) := \sum_{n|N} d_{i-1}(n) \qquad (3\text{–}12)$$

where $d_0(N) = 1$.

Lemma 3.6. *For $l, t \ge 0$ and p prime, we have*

$$d_t(p^l) = \binom{l+t}{t}. \qquad (3\text{–}13)$$

Proof. We work by induction on t. Equality (3–13) is clearly true for $t = 0$ because $d_0(N) = 1$. We then suppose (3–13) is true for $t-1$ where $t \ge 1$. Then

$$d_t(p^l) = \sum_{n|p^l} d_{t-1}(n) = \sum_{i=0}^{l} d_{t-1}(p^i) = \sum_{i=0}^{l}\binom{i+t-1}{t-1}.$$

So $d_t(p^l)$ is the coefficient of x^{t-1} in

$$\begin{aligned}(x+1)^{t-1} + (x+1)^t + \cdots + (x+1)^{l+t-1} \\ &= (x+1)^{t-1}\left(\frac{(x+1)^{l+1}-1}{x}\right) \\ &= \frac{(x+1)^{l+t}-(x+1)^{t-1}}{x}.\end{aligned}$$

Hence $d_t(p^l)$ is the coefficient of x^t in $(x+1)^{l+t} - (x+1)^{t-1}$. Therefore, $d_t(p^l) = \binom{l+t}{t}$. □

Since $d_t(N)$ is a multiplicative function of N, we have

Corollary 3.7. *If $N = p_1^{r_1} \cdots p_s^{r_s}$ where $r_i \geq 1$ and p_i are distinct primes, then*

$$d_t(N) = \prod_{i=1}^{s} \binom{r_i+t}{t}.$$

Lemma 3.8. *For any positive integers N and t, we have*

$$r(N,t) := \begin{cases} 0 & \text{if } N = 1, \\ \sum_{i=1}^{t} (-1)^{t-i}\binom{t}{i} d_{i-1}(N) & \text{if } N > 1. \end{cases} \tag{3–14}$$

Proof. We again prove by induction on t. It is clear from the definition that $r(1,t) = 0$ and $r(N,1) = 1$ for any $t, N \geq 1$. We then suppose $N > 1$ and (3–14) is true for $t-1$ where $t \geq 2$. Then

$$\begin{aligned} r(N,t) &= \sum_{\substack{N_1 \mid N \\ N_1 > 1}} r(N/N_1,\, t-1) \\ &= \sum_{\substack{N_1 \mid N \\ N > N_1 > 1}} r(N/N_1,\, t-1) \\ &= \sum_{N_1 \mid N} \left(\sum_{i=1}^{t-1} (-1)^{t-i-1} \binom{t-1}{i} d_{i-1}(N/N_1) \right) \\ &\quad - \sum_{i=1}^{t-1} (-1)^{t-i-1} \binom{t-1}{i} (d_{i-1}(1) + d_{i-1}(N)) \\ &= \sum_{i=2}^{t} (-1)^{t-i} \binom{t-1}{i-1} d_{i-1}(N) \\ &\quad - \sum_{i=1}^{t-1} (-1)^{t-i-1} \binom{t-1}{i} d_{i-1}(N) + (-1)^{t-1} \\ &= \sum_{i=1}^{t} (-1)^{t-i} \binom{t}{i} d_{i-1}(N) \end{aligned}$$

from (3–12) and the fact that $\binom{t-1}{i-1} + \binom{t-1}{i} = \binom{t}{i}$. □

Corollary 3.9. *The number of cyclotomic polynomials in $\mathcal{L}$ of degree $N-1$, where $N = p_1^{r_1} \cdots p_s^{r_s}, r_i \geq 1$ and the p_i are distinct odd primes, is*

$$4 \sum_{i=1}^{r_1+\cdots+r_s} \sum_{j=1}^{i} (-1)^{i-j} \binom{i}{j} \prod_{k=1}^{s} \binom{r_k+j-1}{j-1}.$$

Proof. From Corollary 3.5, the number of cyclotomic polynomials in $\mathcal{L}$ of degree $N-1$ is

$$4 \sum_{i=1}^{r_1+\cdots+r_s} r(N,i).$$

The corollary now follows from Corollary 3.7 and Lemma 3.8. □

4. CYCLOTOMIC LITTLEWOOD POLYNOMIALS OF ODD DEGREE

We conjecture explicitly that Theorem 3.4 also holds for polynomials of odd degree.

Conjecture 4.1. *A Littlewood polynomial, $P(x)$, of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \pm \Phi_{p_1}(\pm x)\, \Phi_{p_2}(\pm x^{p_1}) \cdots \Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}), \tag{4–1}$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes, not necessarily distinct.

We computed up to degree 210 (except for the case $N-1 = 191$). The computation was based on computing all cyclotomic polynomials with odd coefficients of a given degree and then checking which were actually Littlewood and seeing that this set matched the set generated by the conjecture. For example, for $N-1 = 143$ there are 6773464 cyclotomic polynomials with odd coefficients of which 416 are Littlewood. For $N-1 = 191$ there are 697392380 cyclotomic polynomials with odd coefficients (which was too big for our program).

We can generate all the cyclotomics with odd coefficients from Corollary 2.7 quite easily so the bulk of the work is involved in checking which ones have height 1. The set in the conjecture computes very easily recursively.

Some special cases also support the conjecture. Most notably the case where N is a power of 2. The proof is as follows. From Corollary 2.7, we have

$$P(x) = \Phi_1^{e(1)}(x)\,\Phi_2^{e(2)}(x)\cdots\Phi_{2^{t+1}}^{e(2^{t+1})}(x).$$

Again, we assume $a_0 = a_1 = 1$. Since $\Phi_1(x)\,\Phi_2(x) = x^2 - 1$ and

$$\Phi_{2^l}(x) = \Phi_2(x^{2^{l-1}})$$

for $l \geq 2$, we have $e(2) - e(1) = 1$ and hence

$$P(x) = \Phi_2(x)Q(x^2),$$

for some cyclotomic Littlewood polynomial $Q(x)$. Therefore, by induction, $P(x)$ satisfies (4–1).

ACKNOWLEDGMENT

The authors wish to thank Professor D. Boyd for his advice and support concerning this paper.

REFERENCES

[Borwein 1998] P. Borwein, "Some old problems on polynomials with integer coefficients", pp. 31–50 in *Approximation Theory IX*, edited by C. Chui and L. Schumaker, Vanderbilt University Press, Nashville, TN, 1998.

[Borwein and Erdélyi 1995] P. Borwein and T. Erdélyi, *Polynomials and polynomial inequalities*, Lect. Notes in Math. **161**, Springer, New York, 1995.

[de Bruijn 1948] N. G. de Bruijn, "On Mahler's partition problem", *Nederl. Akad. Wetensch., Proc.* **51** (1948), 659–669. Also appears as *Indagationes Math.* **10** (1948), 210–220.

[Hungerford 1974] T. W. Hungerford, *Algebra*, Holt, Rinehart and Winston, New York, 1974. Reprinted as Graduate Texts in Math. **73**, Springer, Berlin, 1980.

[Lidl and Niederreiter 1983] R. Lidl and H. Niederreiter, *Finite fields*, Second ed., Addison-Wesley, Reading, MA, 1983. Second edition, Cambridge Univ. Press, 1997.

[Littlewood 1968] J. E. Littlewood, *Some problems in real and complex analysis*, Heath Mathematical Monographs, D. C. Heath, Lexington, MA, 1968.

[Mahler 1963] K. Mahler, "On two extremum properties of polynomials", *Illinois J. Math.* **7** (1963), 681–701.

Peter Borwein, Department of Mathematics and Statistics, Simon Fraser University, Burnaby, B.C., Canada V5A 1S6 (pborwein@cecm.sfu.ca)

Kwok-Kwong Stephen Choi, Department of Mathematics, University of British Columbia, Vancouver, B.C., Canada V6T 1Z2 and Department of Mathematics and Statistics, Simon Fraser University, Burnaby, B.C., Canada V5A 1S6 (choi@cecm.sfu.ca)

Received June 3, 1998; accepted in revised form November 28, 1998